AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A method for using digital signatures to validate an amendment to a financial transaction, comprising:

receiving a request to make the amendment to the financial transaction, wherein the financial transaction was previously agreed upon between a first party and a second party, wherein the request is received from a first representative of the first party and includes a suggested change to at least one term of the financial transaction;

validating that the first representative of the first party has permission to agree to the amendment by verifying that the permission information for the first representative is digitally signed by a trusted entity, wherein the permission information is stored in a central permission database;

validating that the first representative of the first party digitally signed the request by using a public key of the first representative to verify that the request was signed by a corresponding private key belonging to the first representative;

if the validation establishes that the first representative signed the request and if the second party desires to agree to the request,

allowing a second representative of the second party to confirm the request by digitally signing the request with a private key belonging to the second representative, and

returning the confirmed request to the first party;

otherwise, if the second party does not desire to agree to the request or if the validation does not establish that the first representative signed the request,

returning a rejection of the request to the first party.

2 (Canceled).

3. (Original) The method of claim 1, further comprising, if the validation establishes that the first representative signed the request, and if the second party does not agree to the request, but instead desires to propose counter-terms, allowing the second party to propose counter-terms by:

creating a responding request including a responding amendment with the counter-terms;

allowing the second representative of the second party to digitally sign the responding request with a private key belonging to the second representative; and

sending the signed responding request to the first party.

4. (Currently amended) The method of claim 3, further comprising:

validating that the second representative of the second party digitally signed the responding request by using a public key of the second representative to verify that the responding request was signed by a corresponding private key belonging to the second representative; and

if the validation establishes that the second representative signed the responding request, and if the first party desires to agree to the responding request,

allowing the first representative of the first party to confirm the responding request by digitally signing the responding request with a private key belonging to the first representative, and

returning the confirmed responding request to the second party;

otherwise, if the first party does not desire to agree to the responding request or if the validation does not establish that the second representative signed the responding request,

returning a rejection of the responding request to the second party.

5. (Original) The method of claim 4, further comprising, prior to allowing the first representative to confirm the responding request, validating that the second representative has permission to agree to the amendment by verifying that permission information for the second representative is digitally signed by a trusted entity.

6. (Original) The method of claim 1, further comprising recording the request and any response to the request in a database.

7. (Original) The method of claim 1, further comprising validating an identity of the first party by using a public key of a certification authority to verify that a certificate containing the public key of the first party was signed by a corresponding private key belonging to the certification authority;

wherein the signing by the certification authority indicates that the certification authority has verified the identity of the first party.

8. (Original) The method of claim 1,

wherein receiving the request from the first party involves receiving the request from a trade facilitator that previously received the request from the first party; and

wherein returning the confirmed request to the first party involves forwarding the confirmed request to the first party through the trade facilitator.

9. (Original) The method of claim 1, wherein prior to receiving the request to make the amendment, the method further comprises, allowing the first representative of the first party to obtain permission to amend the financial transaction by:

sending a request for permission to a first security officer associated with the first party; and

allowing the first security officer to digitally sign a permission record to indicate the first representative has permission to agree to the amendment.

10. (Original) The method of claim 1, wherein the financial transaction involves foreign exchange, and wherein a trade record for the financial transaction includes:

a trade identifier;

an amend trade identifier;

a trade date;

an identifier for a first currency;

a first currency amount;

an identifier for a first organization providing the first currency;

an identifier for a second currency;

a second currency amount; and

an identifier for a second organization providing the second currency.

11. (Currently amended) A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method for using digital signatures to validate an amendment to a financial transaction, the method comprising:

receiving a request to make the amendment to the financial transaction, wherein the financial transaction was previously agreed upon between a first party and a second party, wherein the request is received from a first representative of the first party and includes a suggested change to at least one term of the financial transaction;

validating that the first representative of the first party has permission to agree to the amendment by verifying that the permission information for the first representative is digitally signed by a trusted entity, wherein the permission information is stored in a central permission database;

validating that the first representative of the first party digitally signed the request by using a public key of the first to verify that the request was signed by a corresponding private key belonging to the first representative;

if the validation establishes that the first representative signed the request and if the second party desires to agree to the request,

allowing a second representative of the second party to confirm the request by digitally signing the request with a private key belonging to the second representative, and

returning the confirmed request to the first party;

otherwise, if the second party does not desire to agree to the request or if the validation does not establish that the first representative signed the request,

returning a request rejection to the first party.

12 (Canceled).

13. (Original) The computer-readable storage medium of claim 11, wherein if the validation establishes that the first representative signed the request, and if the second party does not agree to the request, but instead desires to

propose counter-terms, the method further comprises allowing the second party to propose counter-terms by:

creating a responding request including a responding amendment with the counter-terms;

allowing the second representative of the second party to digitally sign the responding request with a private key belonging to the second representative; and

sending the signed responding request to the first party.

14. (Currently amended) The computer-readable storage medium of claim 13, wherein the method further comprises:

validating that the second representative of the second party digitally signed the responding request by using a public key of the second representative to verify that the responding request was signed by a corresponding private key belonging to the second representative; and

if the validation establishes that the second representative signed the responding request, and if the first party desires to agree to the responding request,

allowing the first representative of the first party to confirm the responding request by digitally signing the responding request with a private key belonging to the first representative, and

returning the confirmed responding request to the second party;

otherwise, if the first party does not desire to agree to the responding request or if the validation does not establish that the second representative signed the responding request,

returning a rejection of the responding request to the second party.

15. (Original) The computer-readable storage medium of claim 14, wherein prior to allowing the first representative to confirm the responding request, the method further comprises validating that the second representative has permission to agree to the amendment by verifying that permission information for the second representative is digitally signed by a trusted entity.

16. (Original) The computer-readable storage medium of claim 11, wherein the method further comprises recording the request and any response to the request in a database.

17. (Original) The computer-readable storage medium of claim 11, wherein the method further comprises validating an identity of the first party by using a public key of a certification authority to verify that a certificate containing the public key of the first party was signed by a corresponding private key belonging to the certification authority;

wherein the signing by the certification authority indicates that the certification authority has verified the identity of the first party.

18. (Original) The computer-readable storage medium of claim 11,

wherein receiving the request from the first party involves receiving the request from a trade facilitator that previously received the request from the first party; and

wherein returning the confirmed request to the first party involves forwarding the confirmed request to the first party through the trade facilitator.

19. (Original) The computer-readable storage medium of claim 11, wherein prior to receiving the request to make the amendment, the method further

comprises allowing the first representative of the first party to obtain permission to amend the financial transaction by:

sending a request for permission to a first security officer associated with the first party; and

allowing the first security officer to digitally sign a permission record to indicate the first representative has permission to agree to the amendment.

20. (Original) The computer-readable storage medium of claim 11, wherein the financial transaction involves foreign exchange, and wherein a trade record for the financial transaction includes:

a trade identifier;

an amend trade identifier;

a trade date;

an identifier for a first currency;

a first currency amount;

an identifier for a first organization providing the first currency;

an identifier for a second currency;

a second currency amount; and

an identifier for a second organization providing the second currency.

21. (Currently amended) An apparatus that uses digital signatures to validate an amendment to a financial transaction, comprising:

a receiving mechanism that is configured to receive a request to make the amendment to the financial transaction, wherein the financial transaction was previously agreed upon between a first party and a second party, wherein the request is received from a first representative of the first party and includes a suggested change to at least one term of the financial transaction;

a validation mechanism that is configured to:

validate that the first representative of the first party has permission to agree to the amendment by verifying that the permission information for the first representative is digitally signed by a trusted entity, wherein the permission information is stored in a central permission database; and

~~a validation mechanism that is configured~~ to validate that the first representative of the first party digitally signed the request by using a public key of the first representative to verify that the request was signed by a corresponding private key belonging to the first representative;

an agreement mechanism, wherein if the validation establishes that the first representative signed the request, and if the second party desires to agree to the request, the agreement mechanism is configured to,

allow a second representative of the second party to confirm the request by digitally signing the request with a private key belonging to the second representative, and to

return the confirmed request to the first party;

otherwise, if the second party does not desire to agree to the request or if the validation does not establish that the first representative signed the request, the agreement mechanism is configured to,

return a rejection of the request to the first party.

22 (Canceled).

23. (Original) The apparatus of claim 21, wherein if the validation establishes that the first representative signed the request, and if the second party does not agree to the request, but instead desires to propose counter-terms, the agreement mechanism is configured to:

create a responding request including a responding amendment with the counter-terms;

allow the second representative of the second party to digitally sign the responding request with a private key belonging to the second representative; and to

send the signed responding request to the first party.

24. (Currently amended) The apparatus of claim 23, further comprising:

a second validation mechanism associated with the first party;

wherein the second validation mechanism is configured to validate that the second representative of the second party digitally signed the responding request by using a public key of the second representative to verify that the responding request was signed by a corresponding private key belonging to the second representative; and

a second agreement mechanism associated with the first party;

wherein if the validation establishes that the second representative signed the responding request, and if the first party desires to agree to the responding request, the second agreement mechanism is configured to,

allow the first representative of the first party to confirm the responding request by digitally signing the responding request with a private key belonging to the first representative, and to

return the confirmed responding request to the second party;

otherwise, if the first party does not desire to agree to the responding request or if the validation does not establish that the second representative signed the responding request, the second agreement mechanism is configured to,

return a rejection of the responding request to the second party.

25. (Original) The apparatus of claim 24, wherein prior to allowing the first representative to confirm the responding request, the second validation mechanism is configured to validate that the second representative has permission to agree to the amendment by verifying that permission information for the second representative is digitally signed by a trusted entity.

26. (Original) The apparatus of claim 21, further comprising an archiving mechanism that is configured to record the request and any response to the request in a database.

27. (Original) The apparatus of claim 21, wherein the validation mechanism is configured to validate an identity of the first party by using a public key of a certification authority to verify that a certificate containing the public key of the first party was signed by a corresponding private key belonging to the certification authority;

wherein the signing by the certification authority indicates that the certification authority has verified the identity of the first party.

28. (Original) The apparatus of claim 21,

wherein the receiving mechanism is configured to receive the request from a trade facilitator that previously received the request from the first party; and

wherein the agreement mechanism is configured to return the confirmed request to the first party by forwarding the confirmed request to the first party through the trade facilitator.

29. (Original) The apparatus of claim 21, further comprising a permission obtaining mechanism, wherein prior to receiving the request to make the amendment, the permission obtaining mechanism is configured to:

send a request for permission to a first security officer associated with the first party; and to

allow the first security officer to digitally sign a permission record to indicate the first representative has permission to agree to the amendment.

30. (Original) The apparatus of claim 21, wherein the financial transaction involves foreign exchange, and wherein a trade record for the financial transaction includes:

a trade identifier;

an amend trade identifier;

a trade date;

an identifier for a first currency;

a first currency amount;

an identifier for a first organization providing the first currency;

an identifier for a second currency;

a second currency amount; and

an identifier for a second organization providing the second currency.